HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta/Osasto — Fakultet/Sektion — Faculty	Laitos — Institution — Department
Matemaattis-luonnontieteellinen	Matematiikan ja tilastotieteen laitos

Tekijä — Författare — Author
Vesa Kauhajärvi

Työn nimi — Arbetets titel — Title

Noetherin renkaat ja modulit

Oppiaine — Läroämne — Subject
Matematiikka

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Pro gradu -tutkielma	Lokakuu 2016	25 s.

Tiivistelmä — Referat — Abstract

Pro Gradu-tutkielmassani käsittelen lyhyesti Noetherin modulien ja renkaiden teoriaa ja perusominaisuuksia. Työssäni käyn lävitse niin modulien kuin renkaiden osalta kolme erilaista yleistä tapaa määritellä ne, ja osoitan määritelmien ekvivalenssin. Tämän lisäksi osoitetaan Hilbertin lause. Hilbertin lauseen mukaan polynomirengas $R[X]$ on myös Noetherin rengas, jos R on. Lause yleistetään myös äärellisen monen muuttujan polynomeille.

Tutkielman viimeisessä luvussa osoitan Noetherin renkaan mielivaltaisen ideaalin olevan jaettavissa alkeisideaalien leikkaukseksi, ja totean tämän olevan täysin allegorinen kokonaislukujen alkutekijähajotelmien kanssa.

Avainsanat — Nyckelord — Keywords
algebra, rengas, moduli, Noether, nouseva ketju, äärellisviritteinen

Säilytyspaikka — Förvaringsställe — Where deposited
Kumpulan tiedekirjasto

Muita tietoja — Övriga uppgifter — Additional information

Helsingin Yliopisto
Matemaattis-luonnontieteellinen tiedekunta
Matematiikan ja tilastotieteen laitos

Pro Gradu

Noetherin modulit ja renkaat

Vesa Kauhajärvi

013189125

Ohjaaja: Erik Elfving

23. lokakuuta 2016

Sisältö

Luku 1

Johdanto

Tässä tutkielmassa käsittelen lyhyesti Noetherin modulien ja renkaiden teoriaa. Noetherin renkaat voidaan määritellä nousevan ketjun ehdolla, ja monella muulla tapaa. Tieto siitä, että jokin rengas on Noetherin rengas helpottaa suuresti renkaan muiden algebrallisten ominaisuuksien tutkimista.

Noetherin mukaan nimettyjä äärellisviritteisiä moduleita tutki ensimmäiseksi saksalainen matemaatikko David Hilbert. Hilbert todisti osittain näitä moduleita käyttäen lauseensa, jolle esitän erään todistuksen tämän tutkielman luvussa 4. Hilbertin lauseen mukaan jokainen polynomirengas, jonka kerroinrenkaana on Noetherin rengas, on myös itse Noetherin rengas.

Viimeisessä luvussa tutustutaan alkeishajotelmiin. Osoitamme, että Noetherin renkaiden hajotelmateorialle löytyy hyvin tuttu vastaavuus luonnollisten lukujen alkutekijähajotelmien kanssa.

Noetherin renkaat on nimetty Emmy Noetherin mukaan. Amalie Emmy Noether syntyi 23.03.1882 Erlangenissa Saksassa. Häntä on arvostettu jopa maailmanhistorian tärkeimpänä naismatemaatikkona, mm. Albert Einsteinin toimesta. Hän väitteli matematiikan tohtoriksi 25-vuotiaana Erlangenin yliopistosta. Noether toimi lyhyttä Neuvostoliiton kautta lukuunottamatta Saksassa, kunnes juutalaisena hän joutui siirtymään Adolf Hitlerin noustua valtaan vuonna 1933 Yhdysvaltoihin Princetonin yliopistoon. Ura valtameren takana jäi kuitenkin lyhyeksi, sillä Emmy Noether menehtyi 14.04.1935 kasvaimen poiston komplikaatioihin.

Haluan kiittää kaikkia jotka ovat minua auttaneet tämän Iisakinkirkon kanssa, erityisesti ohjaajaani Erik Elfvingiä.

Luku 2

Määritelmiä

Määrittelemme tässä luvussa jatkoa varten tarvittavat työkalut. Alussa määrittelemme tarvittavat algebralliset rakenteet, ja luvun lopussa käsitellään nousevissa ketjuissa tarvittavaa järjestysteoriaa.

2.1 Algebralliset rakenteet

Tässä kappaleessa määrittelemme käsitteet joita tarvitsemme tulevaisuudessa.

Määritelmä 2.1.1. Olkoon R joukko, jossa on määritelty kaksi operaatiota $+$ ja $\cdot$. Kolmikko $(R, +, \cdot)$ on *rengas*, jos seuraavat ehdot ovat voimassa:

R1 Kaikilla $a, b \in R$ pätee $a + b \in R$.

R2 Kaikilla $a, b, c \in R$ pätee $a + (b + c) = (a + b) + c$.

R3 On olemassa $0 \in R$, jolla on kaikilla $a \in R$ voimassa $a + 0 = 0 + a = a$.

R4 Kaikille $a \in R$ on olemassa $-a$, jolla pätee $a + (-a) = -a + a = 0$.

R5 Kaikilla $a, b \in R$ pätee $a + b = b + a$.

R6 Kaikilla $a, b \in R$ pätee $a \cdot b \in R$.

R7 Kaikilla $a, b, c \in R$ pätee $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

R8 On olemassa $1 \in R$, jolla on kaikilla $a \in R$ voimassa $a \cdot 1 = 1 \cdot a = a$.

R9 Kaikilla $a, b, c \in R$ pätee $a \cdot (b + c) = a \cdot b + a \cdot c$.

R10 Kaikilla $a, b, c \in R$ pätee $(a + b) \cdot c = a \cdot c + b \cdot c$

Siis R on vaihdannainen ryhmä operaation $+$ suhteen (R1-R5), monoidi operaation $\cdot$ suhteen (R6-R8), minkä lisäksi osittelulait R9 ja R10 ovat voimassa. Jos lisäksi kaikilla $a, b \in G$ pätee $a \cdot b = b \cdot a$, sanomme renkaan olevan vaihdannainen. Tällöin osittelulait R9 ja R10 ovat ekvivalentit.

Määritelmä 2.1.2. Vaihdannaista rengasta $(K, +, \cdot)$ jossa $0 \neq 1$ ja pari $(K \setminus \{0\}, \cdot)$ muodostaa vaihdannaisen ryhmän kutsutaan *kunnaksi*. Kunnassa on siis aina vähintään kaksi alkiota.

Seuraava lemma on hyödyllinen muistaa ajatellen kokonaisalueen määritelmää.

Lemma 2.1.3. *Olkoon R rengas, jossa nolla-alkio ja ykkösalkio ovat sama alkio. Tällöin R on nollarengas, eli $R = \{0\}$.*

Todistus. Jos nolla-alkio ja ykkösalkio ovat samat, pätee kaikilla $a \in R$ kertolaskussa $a \cdot 0 = a$. Toisaalta kaikilla $a \in R$ pätee $0 \cdot a = 0$, eli $a = 0$. □

Määritelmä 2.1.4. Olkoon R vaihdannainen rengas, jossa on vähintään kaksi alkiota. Jos kaikilla $a, b \in R$ pätee aina kun $ab = 0$, niin joko $a = 0$ tai $b = 0$ niin rengas R on *kokonaisalue*.

Määritelmä 2.1.5. Olkoon R rengas. Sen osajoukko $I \subset R$ on renkaan R *ideaali*, jos seuraavat ehdot ovat voimassa:

I1 Pari $(I, +)$ on ryhmän $(R, +)$ aliryhmä.

I2 Kaikilla $x \in R$ ja $a \in I$ on voimassa $xa \in I$ ja $ax \in I$.

Jos R on vaihdannainen rengas, riittää luonnollisesti todeta ehto I2 vain toisinpäin. Jos I on renkaan R ideaali ja on voimassa $\varnothing \neq I \subsetneq R$, sanomme, että I on renkaan R *aito ideaali*. Jos ideaali on aito, eikä ole olemassa sellaista ideaalia J jolla pätisi $I \subsetneq J \subsetneq R$, sanomme, että I on *maksimaalinen ideaali*.

Jos ehto I2 on voimassa vain toisinpäin, $ax \in I$, sanomme, että ideaali on vasemmanpuoleinen ideaali. Oikeanpuoleinen ideaali määritellään vastaavalla tapaa. Jos kyseessä on vaihdannainen rengas, kaikki ideaalit ovat sekä vasemman-, että oikeanpuoleisia.

Lemma 2.1.6. *Ideaalikriteeri. Renkaan R osajoukko I on ideaali jos ja vain jos:*

IK1 $0 \in I$

IK2 Kaikilla $a, b \in I$ pätee $a - b \in I$.

IK3 Kaikilla $x \in R$ ja $a \in I$ pätee $xa \in I$ ja $ax \in I$.

Ehto IK3 on sama kuin ideaalin määritelmän ehto I2. Ehdot IK1 ja IK2 seuraavat suoraan ideaalin määritelmän ehdosta I1.

Määritelmä 2.1.7. Olkoot I ja J renkaan R ideaaleja. Määrittelemme ideaalien summan $I + J = \{r \in R \mid r = x + y, x \in I, y \in J\}$. Myös $I + J$ on renkaan R ideaali.

Määritelmä 2.1.8. Olkoon R rengas ja $A \subset R$. Osajoukon A virittämä ideaali on pienin ideaali joka sisältää joukon A. Merkitsemme tätä $\langle A \rangle$. Yhden alkion virittämää ideaalia kutsumme *pääideaaliksi* ja rengasta jonka kaikki ideaalit ovat pääideaaleja kutsumme *pääideaalirenkaaksi*.

Määritelmä 2.1.9. Olkoon R rengas ja $I \subsetneq R$ sen ideaali. Ideaali I on *alkuideaali*, jos kaikilla $x, y \in R$ pätee seuraava ehto: kun $xy \in I$, niin joko $x \in I$ tai $y \in I$. Siis jos tulo xy on ideaalin alkio, ainakin toinen tulon tekijöistä on ideaalin alkio.

Määritelmä 2.1.10. Olkoon R rengas ja $I \subsetneq R$ sen ideaali. Ideaali I on *alkeisideaali*, jos kaikilla $x, y \in R$ pätee seuraava ehto: kun $xy \in I$, niin joko $x \in I$ tai $y^n \in I$ jollain $n \in \mathbb{N}$. Selvästi jokainen alkuideaali on alkeisideaali, sillä alkuideaalit ovat erikoistapaus $n = 1$ alkeisideaaleista.

Lemma 2.1.11. *Jokainen maksimaalinen ideaali on alkuideaali.*

Todistus. Olkoon ideaali $I \subset R$ maksimaalinen, ja oletetaan, ettei se ole alkuideaali. Tällöin on olemassa $a, b \in R \setminus I$, joilla $ab \in I$. Olkoon $J = \langle I \cup \{a\} \rangle = \{x + ar \mid x \in I \wedge r \in R\}$. Selvästi $I \subsetneq J$, joten ideaalin I maksimaalisuuden nojalla $J = R$, ja $1_R \in J$ joten $1_R = x + ar$ joillain $x \in I$ ja $r \in R$. Nyt $b = b1_R = b(x + ar) = bx + bar$. Kuitenkin $bx \in bI \subset RI = I$ ja $bar \in Ir \subset IR = I$, eli $b \in I$, mikä on ristiriidassa oletusten kanssa. Edellisen nojalla ideaali I on alkuideaali. □

Esimerkki 2.1.12. Kokonaislukujen renkaan $(\mathbb{Z}, +, \cdot)$ kaikki ideaalit ovat muotoa $n\mathbb{Z} = \langle n \rangle$, eli ne ovat alkion n virittämiä. Olkoon $I \subset \mathbb{Z}$ ideaali. Ideaalin alkioita ovat siis kaikki kokonaisluvut $\{\cdots, -3n, -2n, -n, 0, n, 2n, \cdots\}$. Oletamme, että $n \in \mathbb{P}$, jossa $\mathbb{P}$ on

alkulukujen joukko, ja $a, b \in \mathbb{Z}$ ovat mielivaltaisia. Nyt jos $ab \in I$, pitää olla joko $a \in I$ tai $b \in I$ sillä jos n jakaa tulon ab, ja koska $n \in \mathbb{P}$, niin n jakaa jommankumman luvuista a tai b. Siis I on alkuideaali.

Jos n ei ole alkuluku eikä 0, ideaali I ei ole alkuideaali. Olkoon $n = pq$, ja $p, q \geqslant 2$. Nyt $pq \in I$, mutta $p \notin I$ ja $q \notin I$.

Erikoistapauksina käsitellään vielä tapaukset $n = 0$ ja $n = 1$. Kokonaislukurengas $\mathbb{Z}$ on tunnetusti kokonaisalue, ja $\langle 0 \rangle = \{0\}$, eli ideaali on alkuideaali. Jos $n = 1$, selvästi $\langle n \rangle = \mathbb{Z}$, eli se ei ole alkuideaali.

Määritelmä 2.1.13. Ideaali I on *jaoton*, jos aina kun I on kahden ideaalin J ja K leikkaus $I = J \cap K$, niin joko $I = J$ tai $I = K$.

Esimerkki 2.1.14. Kokonaislukujen renkaan $(\mathbb{Z}, +, \cdot)$ tapauksessa jaottomat ideaalit vastaavat alkulukujen potensseja. Olkoon $I = \langle pq \rangle = \{\cdots, -2pq, -pq, 0, pq, 2pq, \cdots\}$, jossa $p, q > 1$ ja $p, q \in \mathbb{P}$. Lisäksi oletamme, että $p \neq q$. Nyt $J = \langle p \rangle = \{\cdots, -2p, -p, 0, p, 2p, \cdots\}$ ja $K = \langle q \rangle = \{\cdots, -2q, -q, 0, q, 2q, \cdots\}$. Selvästikin

$$\{\cdots, -2p, -p, 0, p, 2p, \cdots\} \cap \{\cdots, -2q, -q, 0, q, 2q, \cdots\} = \{\cdots, -2pq, -pq, 0, pq, 2pq, \cdots\},$$

eli $I = J \cap K$.

Jos $p = q$, niin $J = K$, ja siis $J \cap K = J = K$.

Toisaalta kaikki ideaalit muotoa $\langle p^n \rangle$, jossa $p \in \mathbb{Z}$ ja $n \in \mathbb{N}$ ovat mielivaltaisia, ovat jaottomia. Jos $\langle p^n \rangle = I \subset J$, pitää ideaalin J olla muotoa $J = \langle p^m \rangle$, missä $m \leqslant n$. Muodostamme kahden ideaalin $I_1 = \langle p^k \rangle$ ja $I_2 = \langle p^l \rangle$ leikkauksen $I_1 \cap I_2$, ja voimme olettaa, että $k < l$. Tällöin selvästi $I_1 \cap I_2 = I_2$. Näin ollen $\langle p^n \rangle$ on jaoton.

Näemme siis, että ideaali on jaoton, jos ja vain jos sen virittää tasan yhden alkuluvun tietty potenssi.

Määritelmä 2.1.15. Määrittelemme kahden ideaalin I ja J *osamääräideaalin* olevan joukon $(I : J) = \{r \in R \mid rJ \subset I\}$.

Lemma 2.1.16. *Renkaan R ideaalien I ja J osamääräideaali $(I : J)$ on myös renkaan R ideaali.*

Todistus. Olkoon $r_1, r_2 \in (I : J)$. Oletimme, että I on ideaali, ja oletusten nojalla myös $r_1 j, r_2 j \in I$. Tällöin kaikilla $j \in J$ pätee $(r_1 + r_2)j = r_1 j + r_2 j \in I$. Siis $(I : J)$ on yhteenlaskun suhteen aliryhmä.

Olkoon $a \in (I : J)$ ja $r \in R$. Nyt mielivaltaisella $j \in J$ pätee $aj \in I$, ja $raj \in I$, sillä I on suljettu kertolaskun suhteen renkaassa R. □

Määritelmä 2.1.17. Olkoon $(G, \cdot)$ ryhmä, ja N sen normaali aliryhmä. Määrittelemme tekijäryhmän $G/N = \{aN \mid a \in G\}$, jossa laskutoimituksena on $(aN) \star (bN) = (a \cdot b)N$ kaikilla $a, b \in G$.

Määritelmä 2.1.18. *Kuvauksen $f : G \longrightarrow H$ ytimen* muodostavat ne $g \in G$, joilla $f(g) = e_H$. Siis ytimen muodostavat ne alkiot, jotka kuvautuvat neutraalialkioon. Merkitsemme tätä $Kerf$.

Määritelmä 2.1.19. Olkoon $(G, \cdot)$ ja $(H, \star)$ ryhmiä. Kuvaus $f : G \longrightarrow H$ on *ryhmähomomorfismi*, jos kaikilla ryhmien alkioilla pätee $f(x \cdot y) = f(x) \star f(y)$.

Määritelmä 2.1.20. Olkoon $(G, \cdot)$ ja $(H, \star)$ ryhmiä. Kuvaus $f : G \longrightarrow H$ on *ryhmäisomorfismi*, jos se on bijektio, ja sekä f, että f^{-1} ovat ryhmähomomorfismeja. Jos rakenteet G ja H ovat isomorfisia, merkitsemme $G \cong H$.

Lause 2.1.21. *Ryhmien homomorfialause. Olkoon $(G, \cdot)$ ja $(H, \star)$ ryhmiä, ja $f : G \longrightarrow H$ ryhmähomomorfismi. Tällöin tekijäryhmä $G/Kerf \cong Im(f)$.*

Todistus. Muodostamme kuvauksen $g : G/Kerf \longrightarrow Im(f), aKerf \mapsto f(a)$ ja väitämme, että se on hyvinmääritelty ja bijektiivinen. Olkoon $a, b \in G$. Jos alkioiden a ja b määräämät sivuluokat ovat samat, niin $a \in bKerf$, eli $a = bk$ jollakin $k \in Kerf$. Nyt

$$g(a(Kerf)) = f(a) = f(bk) = f(b)f(k) = f(b) \cdot 1 = f(b) = g(b(Kerf)),$$

siis g on hyvinmääritelty.

Tutkitaan seuraavaksi alkioiden a ja b muodostamia ytimen sivuluokkia $(a(Kerf))$ ja $(b(Kerf))$. Nyt

$$g\Big((a(Kerf))(b(Kerf))\Big) = g(ab(Kerf)) = f(ab) = f(a)f(b) = g(a(Kerf))g(b(Kerf)).$$

Ryhmähomomorfismi on injektio jos ja vain jos $Kerf = e_{G/Kerf}$. Jos $g(a(Kerf)) = e_H$, niin $f(a) = e_H$, eli $a \in Kerf$, mistä seuraa $a(Kerf) = Kerf = e_{G/Kerf}$, ja siis g on injektio. Kuvaus g on myös surjektio, sillä

$$\bigcup_{a \in G} f(a) = f(G) = Imf.$$

Siis g on isomorfismi. □

Määritelmä 2.1.22. Joukon X kaksipaikkainen relaatio $\sim$ on ekvivalenssirelaatio, jos se täyttää seuraavat ehdot:

Refleksiivisyys: $a \sim a$ kaikilla $a \in X$.

Symmetrisyys: kaikilla $a, b \in X$ jos $a \sim b$, niin $b \sim a$.

Transitiivisuus: kaikilla $a, b, c \in X$ jos $a \sim b$ ja $b \sim c$, niin $a \sim c$.

Määrittelemme joukossa X alkion a ekvivalenssiluokan $[a] = \{b \in X \mid a \sim b\}$.

Määritelmä 2.1.23. Olkoon R rengas, jonka ei tarvitse olla vaihdannainen. Vaihdannainen ryhmä $(M, +)$ on renkaan *vasemmanpuoleinen moduli* jos kaikilla $r, s \in R$ ja $x, y \in M$ operaatio $R \times M \longrightarrow M$ on määritelty ja se täyttää seuraavat ehdot:

M1 $r(x + y) = rx + ry$

M2 $(r + s)x = rx + sx$

M3 $(ab)x = a(bx)$

M4 $1x = x$

Modulia M, jonka kerroinrengas on R, nimitetään R-moduliksi. Oikeanpuoleiset modulit määritellään vastaavalla tapaa.

Lause 2.1.24. *Modulien homomorfialause. Olkoon M ja N R-moduleita, ja $h : M \longrightarrow N$ modulihomomorfismi. Tällöin tekijämoduli $M/Kerh \cong Im(h)$.*

Todistus. Olkoon $m \in M$. Isomorfismi h määritellään $m + Kerh \mapsto h(m)$. Todistus on tästä eteenpäin käytännössä identtinen ryhmien homomorfialauseen todistuksen kanssa. □

Lause 2.1.25. *Renkaan $(R, +, \cdot)$ jokainen ideaali I on $R-$moduli, operaatioina renkaan yhteen- ja kertolasku.*

Todistus. Pari $(R, +)$ on renkaan määritelmän nojalla vaihdannainen ryhmä, ja $(I, +)$ on sen aliryhmänä myös vaihdannainen ryhmä. Renkaan kertolasku $R \times I \longrightarrow I$ täyttää modulin määritelmän ehdot. □

Määritelmä 2.1.26. Olkoon M R-moduli. Modulin M aliryhmä N on *alimoduli*, jos se on suljettu modulin yhteenlaskun ja skalaarikertolaskun suhteen. Pitää siis päteä seuraavat ehdot kaikilla $x, y \in N$ ja $a \in R$:

AM1 $N \neq \varnothing$

AM2 $x - y \in N$

AM3 $ax \in N$.

Määritelmä 2.1.27. Olkoon R rengas, M R-moduli, ja N modulin M alimoduli. Määrittelemme modulien M ja N *tekijämodulin* M/N ekvivalenssirelaatiolla $\sim_N$, jolla $a \sim_N b$ jos ja vain jos $b - a \in N$. Tekijämodulin M/N alkiot ovat ekvivalenssirelaation ekvivalenssiluokat $\{x + N \mid x \in M\}$. Laskutoimituksena on $(x + N) + (y + N) = x + y + N$, ja kertolaskuna skalaarikertolasku.

Määritelmä 2.1.28. Olkoon M R-moduli, ja $S \subset M$, ja S on äärellinen. Summa

$$\sum_{x \in S} r_x x$$

on joukon S alkioiden *lineaarikombinaatio*. Joukko $\{r_x\}_{x \in S}$ koostuu joukon R alkioista, joita kutsutaan kertoimiksi.

Olkoon N kaikkien joukon S lineaarikombinaatioiden joukko. Tällöin N on modulin M alimoduli, sillä jos

$$\sum_{x \in S} r_x x \text{ ja } \sum_{x \in S} p_x x$$

ovat kaksi lineaarikombinaatiota, niiden summa on

$$\sum_{x \in S} (r_x + p_x) x,$$

ja jos $a \in R$, niin

$$a \sum_{x \in S} r_x x = \sum_{x \in S} a r_x x.$$

Kutsumme modulia N joukon S virittämäksi, ja joukkoa S modulin N kannaksi. Jos modulin M jokin kanta on äärellinen, kutsumme modulia *äärellisviritteiseksi*.

Määritelmä 2.1.29. Olkoon $(M_i)_{i\in I}$ mielivaltainen perhe R-moduleja. Modulien (M_i) *suora tulo* koostuu alkioperheistä $x = (x_i)_{i\in I}$, missä $x_i \in M_i$ kaikilla $i \in I$. Suoraa tuloa merkitään $\prod_{i\in I} M_i$. Suora tulo on R-moduli, kun laskutoimitukset määritellään pisteittäin seuraavalla tapaa:

- $(x + y)_i = x_i + y_i$ ja
- $(ax)_i = ax_i$

kaikilla $x, y \in \prod_{i\in I} M_i, i \in I$ ja $a \in \mathbb{R}$.

Määritelmä 2.1.30. Moduleille voidaan määritellä myös *suora summa*, joka on vastaava konstruktio kuin suora tulo, mutta lisävaatimuksena $x_i \neq 0$ vain äärellisellä määrällä indeksejä. Suora summa on R-moduli, kun laskutoimitukset määritellään kuten suorassa tulossa. Suoraa summaa merkitään $\bigoplus_{i\in I} M_i$.

Määritelmä 2.1.31. Olkoon R rengas, M vasemmanpuoleinen R-moduli, ja $\varnothing \neq S \subset M$. Kutsumme osajoukon S *annihilaattoriksi* $Ann_R(S)$ niiden alkioiden $r \in R$ joukkoa, joilla kaikilla $s \in S$ pätee $rs = 0$. Siis $Ann_R(S) = \{r \in R \mid \forall s \in S : rs = 0\}$

Määritelmä 2.1.32. Kutsumme R-modulia M *alkumoduliksi*, jos mielivaltaiselle epätyhjälle alimodulille $N \subset M$ pätee $Ann_R(M) = Ann_R(N)$.

Määritelmä 2.1.33. Määrittelemme R-modulin M *liittoalkuideaalin* $Ass_R(M)$ olemaan ideaali muotoa $Ann_R(N)$, jossa $N \subset M$ on modulin M alkumoduli.

2.2 Järjestykset

Määritelmä 2.2.1. Joukon A relaatio $\leqslant$ on *osittainen järjestys*, jos kaikilla $a, b, c \in A$ pätee seuraavat ehdot:

J1. $a \leqslant a$, eli *refleksiivisyys*.

J2. Jos $a \leqslant b$ ja $b \leqslant a$, niin $a = b$, eli *antisymmetrisyys*.

J3. Jos $a \leqslant b$ ja $b \leqslant c$, niin $a \leqslant c$, eli *transitiivisuus*.

Jos lisäksi pätee seuraava ehto, järjestys on *täysi*.

J4. Jos $a, b \in A$, niin joko $a \leqslant b$ tai $b \leqslant a$.

Alkiota x jolle ei ole olemassa alkiota $a \in A$ niin, että $x < a$ kutsumme maksimaaliseksi alkioksi. Siis millään alkiolla a ei päde, että a olisi aidosti isompi kuin x.

Joukon A alkiota y jolle kaikilla $b \in A$ pätee $b \leqslant y$ kutsumme joukon A ylärajaksi.

Määritelmä 2.2.2. Olkoon $C \subset A$ osittain järjestetyn joukon osajoukko. Osittainen järjestys $\leqslant$ indusoi jokaiseen A:n osajoukkoon järjestyksen. Jos C:n järjestys on täysi, C on *ketju* A:ssa.

Lause 2.2.3. *Zornin lemma. Olkoon $(P, \leqslant)$ epätyhjä osittain järjestetty joukko, niin, että jokaisella P:n ketjulla C on yläraja joukossa P. Tällöin joukossa P on ainakin yksi maksimaalinen alkio.* Zornin lemma on ekvivalentti hyvinjärjestyslauseen ja valinta-aksiooman kanssa.[1]

Määritelmä 2.2.4. Sanomme, että osittain järjestetty joukko täyttää *nousevan ketjun ehdon*, jos jokainen ketju C on ylhäältä päin rajoitettu. Yhtäpitävästi, olkoon $\cdots \leqslant a_1 \leqslant a_2 \leqslant a_3 \leqslant \cdots$ ketju joukon C alkioita. Tällöin on olemassa $x \in \mathbb{R}$, josta alkaen kaikilla $y \geqslant x$ pätee $a_x = a_y$. Tulee huomata, että ketju voi siis olla ylinumeroituvasti indeksöity, ja alkioiden a_1 ja a_2 välissä voi olla mielivaltainen määrä alkioita.

Luku 3

Noetherin renkaat ja modulit

Luvussa määrittelemme niin Noetherin modulit kuin renkaat kolmella eri tavalla, ja osoitamme kaikki määritelmät ekvivalenteiksi. Lopuksi käymme läpi joitakin esimerkkejä molemmista.

3.1 Noetherin moduli

Moduli M on *Noetherin R-moduli* jos se täyttää minkä tahansa seuraavista kolmesta ehdosta:

1. Jokaisella alimodulilla on äärellinen kanta.

2. Jokainen modulin M nouseva ketju alimoduleja $M_1 \subset M_2 \subset M_3 \subset \cdots$ sisältää sellaisen alimodulin M_k, jolla kaikilla $n > k$ pätee $M_k = M_n$. Siis ketjun toisistaan eroavien alkioiden määrä on äärellinen, eli M täyttää nousevan ketjun ehdon.

3. Jokaisessa epätyhjässä alimodulien muodostamassa joukossa X on ainakin yksi maksimaalinen alkio M_0. Siis jos $N \in X$ ja $M_0 \subset N$, niin $N = M_0$.

Lause 3.1.1. *Ehdot* $1 - 3$ *ovat keskenään ekvivalentteja.*

Todistus. Osoitamme ehdot ekvivalenteiksi järjestyksessä $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$.

3.1.1 $1 \Rightarrow 2$

Olkoon $M_1 \subset M_2 \subset M_3 \subset \cdots$ nouseva ketju modulin M alimoduleja. Merkitään

$$M_\infty = \bigcup_{n=1}^{\infty} M_n$$

Alimodulien yhdiste ei yleisesti ottaen ole välttämättä alimoduli, mutta tässä tapauksessa M_∞ on alimoduli, koska alimodulit ovat sisäkkäisiä. Osoitetaan tämä vielä kohta kohdalta käymällä läpi alimodulin ehdot.

AM1. M_1 on alimoduli ja määritelmän nojalla epätyhjä. Lisäksi pätee $M_1 \subset M_\infty$ joten alimoduli M_∞ on epätyhjä.

AM2. Otetaan mielivaltaiset $x, y \in M_\infty$. Nyt on olemassa indeksi $i \in \mathbb{N}$, jolla $x \in M_i$ ja $j \in \mathbb{N}$, jolla $y \in M_j$. Sisäkkäisyyden nojalla pätee joko $M_i \subset M_j$ tai $M_j \subset M_i$. Voimme olettaa jälkimmäisen vaihtoehdon olevan voimassa ilman, että todistus kärsii. Nyt siis $x, y \in M_i$, ja koska M_i on alimoduli, niin $x - y \in M_i$. Nyt koska $M_1 \subset \cdots \subset M_i \subset \cdots \subset M_\infty$ pätee $x - y \in M_\infty$.

AM3. Otetaan mielivaltainen $x \in M_\infty$ ja $a \in R$. Nyt on olemassa indeksi $i \in \mathbb{N}$, jolla $x \in M_i$, eli $ax \in M_i$. Samoin kuten edellä $M_1 \subset \cdots \subset M_i \subset \cdots \subset M_\infty$ pätee, että $ax \in M_\infty$.

Nyt ehdon 1 nojalla on olemassa äärellinen joukko $x_1, x_2, \cdots, x_m$ joka on joukon M_∞ kanta. Jokainen x_i kuuluu johonkin alimoduliin M_j, joten on olemassa indeksi $n \in \mathbb{N}$ jolla $x_1, x_2, \cdots, x_m \in M_n$. Tällöin pätee $\langle x_1, x_2, ..., x_r \rangle \subset M_n \subset M_\infty = \langle x_1, x_2, ..., x_r \rangle$, mikä todistaa väitteen. Ketjun modulit ovat siis samoja jostain indeksistä $j \in \mathbb{N}$ alkaen.

3.1.2 $2 \Rightarrow 3$

Oletetaan, että on olemassa epätyhjä joukko S alimoduleja, jossa ei ole maksimaalista alkiota. Olkoon $M_1 \in S$ mielivaltainen. Koska se ei ole maksimaalinen alkio, on olemassa M_2, jolle pätee $M_1 \subsetneq M_2$. Jos joukkoa M_2 ei ole olemassa, M_1 on maksimaalinen. Voimme jatkaa vastaavaa päättelyä, ja muodostaa äärettömän nousevan ketjun $M_1 \subset M_2 \subset M_3 \subset \cdots$, mikä on ristiriita ehdon 2 kanssa.

3.1.3 $3 \Rightarrow 1$

Oletetaan, että on olemassa alimoduli N jolla ei ole äärellistä kantaa. Olkoon S kaikkien modulin N äärellisviritteisten alimodulien joukko. Ehdon 3 nojalla joukolla S on maksimaalinen alkio M_n. Tällöin M_n on äärellisviritteinen ja $M_n \subset N$. Koska N ei ole äärellisviritteinen, on olemassa $a \in N \setminus M_n$. Muodostamme modulin $M_k = M_n + Ra$, jolloin M_k on aidosti isompi kuin M_n, mikä on ristiriidassa sen oletuksen kanssa, että M_n olisi maksimaalinen. □

Lemma 3.1.2. *Olkoon R rengas, ja M Noetherin R-moduli. Jokainen modulin M alimoduli ja tekijämoduli on Noetherin moduli.*

Todistus. Alimodulien suhteen lause on selvä Noetherin modulin määritelmän ensimmäisen kohdan nojalla.

Olkoon N modulin M alimoduli, ja $f : M \longrightarrow M/N$ kanoninen homomorfismi $f(x) = [x]$. Olkoon $\overline{M_1} \subset \overline{M_2} \subset \cdots$ nouseva ketju tekijämodulin M/N alimoduleja, ja määritellään $M_i = f^{-1}(\overline{M_i})$. Nyt $M_1 \subset M_2 \subset \cdots$ on nouseva ketju modulin M alimoduleja. Noetherin modulin määritelmän nojalla tällä ketjulla on maksimaalinen alkio M_r, eli $M_k = M_r$ ja siis $\overline{M_k} = \overline{M_r}$ kaikilla $k \geqslant r$. Nyt siis $f(M_r) = \overline{M_r}$, mistä väite seuraa. □

Lemma 3.1.3. *Olkoon M moduli, ja N edellisen alimoduli. Oletetaan, että N ja M/N ovat Noetherin moduleja. Tällöin myös M on Noetherin moduli.*

Todistus. Määritellään modulin M jokaista alimodulia L kohti pari moduleja $(L \cap N, (L + N)/N)$, joita kutsumme myöhemmin apumoduleiksi. Olkoot $E \subset F$ modulin M alimoduleja. Nyt jos alimodulien E ja F apumodulit ovat samat, niin $E = F$. Tämä nähdään seuraavasta. Oletetaan, että $x \in F$. Nyt jos $(E + N)/N = (F + N)/N$ on olemassa alkiot $u, v \in N$ ja $y \in E$, joilla $y + u = x + v$. Tällöin $x - y = u - v \in F \cap N = E \cap N$. Koska $y \in E$, seuraa, että $x \in E$, mikä todistaa väitteen.

Otamme mielivaltaisen nousevan ketjun modulin M alimoduleja $E_1 \subset E_2 \subset \cdots$. Nyt myös alimoduleihin E_i liittyvät apumodulit muodostavat nousevat ketjut alimoduleja alimodulin N ja tekijämodulin M/N suhteen. Oletimme, että N ja M/N ovat Noetherin moduleja, joten nämä ketjut pysähtyvät johonkin alkioon. Edellisestä seuraa, että myös ketju $E_1 \subset E_2 \subset \cdots$ pysähtyy. □

Lemma 3.1.4. *Jos N ja L ovat Noetherin moduleita, myös niiden suora summa $N \oplus L$ on. Äärellinen suora summa Noetherin moduleista on Noetherin moduli.*

Todistus. Suora summa $N \oplus L$ on Noetherin moduli, sillä N on sen alimoduli, ja $(N \oplus L)/N$ on isomorfinen alimodulin L kanssa, ja lemman 3.1.3 nojalla myös N on Noetherin moduli. Muodostamme surjektiivisen homomorfismin $f : N \times L \longrightarrow N \oplus L, f(x, y) = (x + y)$. Lemman 3.1.2 nojalla myös $N \oplus L$ on Noetherin moduli. Operaation voi toistaa äärellisen monta kertaa, joten edellinen pätee kaikille äärellisille suorille summille. □

3.2 Noetherin rengas

Rengas R on *vasemmanpuoleinen Noetherin rengas*, jos mikä tahansa seuraavista ehdoista on voimassa:

1. Jokainen renkaan vasemmanpuoleinen ideaali I on äärellisviritteinen, siis on olemassa alkiot $a_1, a_2, \cdots, a_n \in I$ joille pätee $I = a_1R + a_2R + \cdots + a_nR$.
2. Jokainen nouseva epätyhjä ketju renkaan vasemmanpuoleisia ideaaleja osittain järjestettynä sisältyvyysrelaation mukaan sisältää maksimaalisen alkion. Toisin sanoen R täyttää nousevan ketjun ehdon.
3. Jokaisessa epätyhjässä joukossa renkaan R vasemmanpuoleisia ideaaleja on maksimaalinen alkio.

Oikeanpuoleinen Noetherin rengas määritellään vastaavalla tapaa, ja todistukset ovat muuten identtisiä. Vaihdannaisten renkaitten tapauksessa vasemman- ja oikeanpuoleiset renkaat ovat identtisiä.

Lause 3.2.1. *Ehdot* $1 - 3$ *ovat ekvivalentteja keskenään.*

Todistus. Osoitamme lauseet ekvivalenteiksi keskenään järjestyksessä $1 \Rightarrow 2 \Rightarrow 1$ ja $2 \Rightarrow 3 \Rightarrow 2$.

3.2.1 $1 \Rightarrow 2$

Muodostetaan ketju ideaaleja $I_1 \subset I_2 \cdots$, jolloin

$$J = \bigcup_{i \geqslant 1} I_i$$

on myös ideaali. Ideaali J on oletuksen 1 nojalla joukon $\{a_1, a_2, \cdots a_n\}$ virittämä. Ketju on nouseva, joten $\{a_1, a_2, \cdots a_n\} \subset I_k$ jollain $k \in \mathbb{N}$. Selvästi $\langle a_1, a_2, \cdots a_n \rangle = J = I_k$, jolloin kaikilla $m \geqslant k$ pätee $I_k = I_m$.

3.2.2 $2 \Rightarrow 1$

Oletetaan, että on olemassa ideaali I joka ei ole äärellisviritteinen, siis millään joukolla $A = \{a_1, a_2, \cdots a_n\}$, missä $n \in \mathbb{N}$, A:n virittämä ideaali ei ole I. Muodostetaan ketju $\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \cdots$. Tämä ketju ei sisällä maksimaalista alkiota.

3.2.3 $2 \Rightarrow 3$

Valitaan mielivaltainen joukko vasemmanpuoleisia ideaaleja. Järjestetään ideaalit ketjuihin sisältyvyysrelaation suhteen. Jokaisella ketjulla on maksimaalinen alkio.

3.2.4 $3 \Rightarrow 2$

Muodostetaan nouseva ketju ideaaleja $I_1 \subset I_2 \cdots$. Oletuksen nojalla joukossa on maksimaalinen alkio I_n. Koska kaikilla $m \geqslant n$ pätee $I_m \geqslant I_n$, pitää olla $I_n = I_{n+1} = \cdots$.
Näin ollen kaikki kolme määritelmää on todistettu ekvivalenteiksi. □

3.3 Esimerkkejä

Esimerkki 3.3.1. Jokainen moduli, jossa on äärellinen määrä alkioita, on selvästi Noetherin moduli.

Esimerkki 3.3.2. Kokonaislukujen joukko $\mathbb{Z}$ on Noetherin $\mathbb{Z}-$moduli, sillä $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$, ja jokainen alimoduli on kokonaislukujoukon $\mathbb{Z}$ aliryhmä, ja siis äärellisviritteinen, kuten kaikki joukon $\mathbb{Z}$ aliryhmät.

Esimerkki 3.3.3. Mikä tahansa äärellisviritteinen moduli, jonka kerroinrenkaana on Noetherin rengas, on Noetherin moduli.

Todistus. Olkoon R Noetherin rengas, ja $x_1, x_2, \cdots, x_n$ $R-$modulin M virittäjät. Voimme muodostaa homomorfismin

$$f : \underbrace{R \times R \times \cdots \times R}_{\text{n kertaa}} \longrightarrow M, f(a_1, a_2, \cdots, a_n) = a_1x_1 + a_2x_2 + \cdots + x_na_n.$$

Homomorfismi f on surjektio, koska alkiot $x_1, x_2, \cdots, x_n$ virittävät modulin M. Lemman 3.1.4 nojalla äärellinen karteesinen tulo on Noetherin moduli. Kuvaus f on surjektio. Lemman 3.1.2 nojalla $(R \times R \times \cdots \times R)/Kerf$ tekijämodulina on Noetherin moduli, ja

edelleen lauseen 2.1.21 nojalla $(R \times R \times \cdots \times R)/Kerf \cong M$ eli siis myös M on Noetherin moduli lauseen 2.1.24 nojalla. □

Esimerkki 3.3.4. Jokainen kunta on Noetherin rengas, sillä kunnassa on aina vain kaksi ideaalia.

Esimerkki 3.3.5. Jokainen pääideaalirengas, kuten kokonaislukujen joukko $(\mathbb{Z}, +, \cdot)$, on Noetherin rengas. Renkaan jokainen ideaali on yhden alkion virittämä, sillä ryhmän $(\mathbb{Z}, +)$ jokainen aliryhmä on muotoa $n\mathbb{Z} = \langle n \rangle$. Kohdan 3.2 pykälän 1. nojalla $(\mathbb{Z}, +, \cdot)$ on Noetherin rengas.

Esimerkit renkaista jotka eivät ole Noetherin renkaita ovat monimutkaisempia.

Esimerkki 3.3.6. Äärettömän monen muuttujan polynomirengas $R[X_1, X_2, \cdots]$ ei ole Noetherin rengas, sillä ideaalien jono $\langle X_1 \rangle \subset \langle X_1, X_2 \rangle \subset \langle X_1, X_2, X_3 \rangle, \cdots$ on selvästi nouseva, mutta sillä ei ole maksimaalista alkiota.

Luku 4

Polynomirenkaat ja Hilbertin lause

Luvussa määrittelemme polynomirenkaat, ja todistamme Hilbertin lauseen. Hilbertin lauseen mukaan mikä tahansa polynomirengas, jossa kerroinrenkaana on Noetherin rengas, on myös Noetherin rengas. Lopuksi yleistetään tulos äärelliselle määrälle muuttujia.

Määritelmä 4.0.7. *Polynomirengas.* Olkoon R vaihdannainen rengas. Määrittelemme yhden tuntemattoman R-kertoimisen polynomin äärettömänä summana

$$a = \sum_{k=0}^{\infty} a_k X^k = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \cdots ,$$

jossa $a_k \in R$ kaikilla $k \in \mathbb{N}$, ja jollain indeksillä $n \in \mathbb{N}$ pätee kun $m > n$, niin $a_m = 0$. Siis polynomissa on vain äärellinen määrä nollasta eroavia termejä. Renkaan alkioita a_k kutsumme kertoimiksi. Merkitsemme $R[X]$ kaikkien R-kertoimisten polynomien joukkoa.

Polynomin aste on se suurin indeksi i, jonka kerroin ei ole nolla. Polynomin f astetta merkitään $deg(f)$.

Polynomien summa määritellään

$$a + b = \sum_{k=0}^{\infty} a_k X^k + \sum_{k=0}^{\infty} b_k X^k = \sum_{k=0}^{\infty} (a_k + b_k) X^k$$

ja tulo

$$ab = \left(\sum_{k=1}^{\infty} a_k X^k \right) \left(\sum_{k=0}^{\infty} b_k X^k \right) = \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i b_j \right) X^k$$

Lause 4.0.8. *Jos rengas R on kokonaisalue, myös polynomirengas $R[X]$ on kokonaisalue. Kaikilla polynomeilla $f, g \in R[X]$ pätee tällöin $deg(fg) = deg(f) + deg(g)$.*

Todistus. Olkoon $f = a_0 + a_1X + \cdots + a_mX^m$ ja $g = b_0 + b_1X + \cdots + b_nX^n$. Nyt $deg(f) = m$ ja $deg(g) = n$. Lasketaan polynomien tulo $fg = a_0b_0 + (a_0b_1 + a_1b_0)X + \cdots + a_mb_nX^{m+n}$, ja määrittelimme $a_m \neq 0$ ja $b_n \neq 0$. Koska R on kokonaisalue, niin $a_mb_n \neq 0$. Tämän nojalla $fg \neq 0$ ja polynomin fg aste on todella $m + n$. □

Lause 4.0.9. *Hilbertin lause. Jos rengas R on Noetherin rengas, tällöin myös $R[X]$ on Noetherin rengas. Jos R on vasemman- tai oikeanpuoleinen Noetherin rengas, $R[X]$ on samanpuoleinen Noetherin rengas kuin R.*

Todistus. Käsittelemme ensin Noetherin renkaan tapauksen, ja palaamme lopuksi vasemman- ja oikeanpuoleisiin tapauksiin.

Olkoon $J \subset R[X]$ ideaali. Määritellään I_i käsittämään 0 ja sellaiset alkiot $a \in R$, jotka ovat jonkin polynomin suurimpia kertoimia $a_0 + a_1X + \cdots + a_{i-1}X^{i-1} + aX^i \in J$.

Nyt myös I_i on ideaali, sillä jos $a, b \in I_i$, niin $a - b \in I$, sillä ideaalikriteerin nojalla

$$a_0 + a_1X + \cdots + a_{i-1}X^{i-1} + aX^i - (b_0 + b_1X + \cdots + b_{i-1}X^{i-1} + bX^i)$$

$$= (a_0 - b_0) + (a_1 - b_1)X + \cdots + (a_{i-1} - b_{i-1})X^{i-1} + (a - b)X^i \in J.$$

Lisäksi jos a on polynomin f korkeinta astetta olevan termin kerroin, ja $r \in R$, niin $rf \in J$. Polynomin rf korkeinta astetta olevan termin kertoja on ra, eli $ra \in I_i$.

Voimme muodostaa nousevan ketjun ideaaleja $I_0 \subset I_1 \subset I_2 \subset \cdots$. Todistetaan ketjun nousevuus. Olkoon $m < n$. Ei siis tarvitse olla $n = m + 1$. Osoitamme, että $I_m \subset I_n$. Nyt olkoon $x_m \in I_m$ mielivaltainen ideaalin I_m alkio, eli on olemassa polynomi $a_0 + a_1X + \cdots + x_mX^m \in J$. Koska J on ideaali, tulo $(X^{n-m})(a_0 + a_1X + \cdots + x_mX^m) \in J$, eli $x_m \in I_n$, mikä todistaa asian. Noetherin renkaiden määritelmän nojalla jostain indeksistä $r \in \mathbb{N}$ alkaen $I_r = I_{r+1}$.

Olkoon $a_{01}, a_{02}, \cdots, a_{0n_0}$ ideaalin I_0 virittäjät, $a_{11}, a_{12}, \cdots, a_{1n_1}$ ideaalin I_1 virittäjät, jne. ja $a_{r1}, a_{r2}, \cdots, a_{rn_r}$ ideaalin I_r virittäjät. Nyt jokaisella $i = 0, \cdots, r$ ja $j = 1, \cdots, n_i$ olkoon f_{ij} polynomi, joka on ideaalin J alkio, asteena i ja suurimpana kertoimena a_{ij}.

Osoitamme, että polynomien f_{ij} joukko virittää ideaalin J.

Olkoon $f \in J$, ja $deg(f) = d$. Osoitamme, että $f \in \langle f_{ij} \rangle$. Oletetaan, että $d \geqslant 0$. Jos $d > r$, niin suurimmat kertoimet polynomeista

$$X^{d-r}f_{r1}, X^{d-r}f_{r2}, \cdots, X^{d-r}f_{rn_r}$$

virittävät ideaalin I_d. Voimme valita alkiot $x_1, x_2, \cdots, x_{n_r} \in R$ joilla polynomin

$$g = f - x_1 X^{d-r} f_{r1} - x_2 X^{d-r} f_{r2} - \cdots - x_{n_r} X^{d-r} f_{rn_r}$$

aste on aidosti pienempi kuin d, ja $g \in J$.

Osoitamme, että alkiot $x_1, x_2, \cdots, x_{n_r}$ ovat olemassa. Huomaamme ensin, että koska $d > r$, ja I_r oli ideaaliketjun viimeinen alkio, $I_d = I_r$. Tiedämme, että $a \in I_d = I_r$. Lisäksi tiedämme, että alkiot $a_{r1}, a_{r2}, \cdots, a_{rn_r}$ virittävät ideaalin I_r, ja löytyy $x_1, x_2, \cdots, x_{n_r}$, joilla $a = x_1 a_{r1} + x_2 a_{r2} + \cdots + x_{n_r} a_{rn_r}$.

Jos $d \leqslant r$, voimme vähentää lineaarisen kombinaation

$$f - c_1 f_{d1} - c_2 f_{d2} - \cdots - c_{n_d} f_{dn_d} = h,$$

jolloin saamme polynomin jonka aste on aidosti pienempi kuin d, ja $h \in J$. Nyt siis polynomi jonka olemme vähentäneet polynomista f sisältyy ideaaliin, jonka f_{ij} virittää. Voimme nyt ottaa induktion nojalla polynomin $h \in \langle f_{ij} \rangle$, ja toistaa operaation äärellisen monta kertaa, ja pääsemme tilanteeseen $f - h = 0$.

Edellä on käsitelty Noetherin renkaan tapaus. Todistus on helppo muokata tarvittaessa vasemman- tai oikeanpuoleiseksi, kertolaskuissa tarvitsee vaihtaa tekijöiden järjestystä. Muuten todistus menee täysin samalla tavalla. □

Lause 4.0.10. *Hilbertin lause useamman muuttujan polynomeille. Jos rengas R on Noetherin rengas, tällöin myös $R[X_1, X_2, \cdots, X_n]$ on Noetherin rengas.*

Todistus. Voimme toistaa lauseen 4.0.9 päättelyn n kertaa, mikä riittää osoittamaan asian. □

Tulee huomata, että lauseessa 4.0.10 luvun n tulee olla äärellinen. Äärettömän monen muuttujan tapauksessa niiden virittämä ideaali ei olisi äärellisviritteinen.

Luku 5

Alkeishajotelmat

Viimeisessä luvussa käsittelemme alkeishajotelmien teoriaa. Osoitamme, että missä tahansa Noetherin renkaassa jokainen ideaali voidaan ilmaista jaottomien ideaalien leikkauksena, ja osoitetaan tämän olevan yleistys luonnollisten lukujen alkutekijöihin jakamisesta.

Lemma 5.0.11. *Jokainen jaoton ideaali Noetherin renkaassa R on alkeisideaali.*

Todistus. Oletetaan, että ideaali I on jaoton, ja $ab \in I$. Osoitamme, että joko $a \in I$ tai, että $b^n \in I$ jollain $n \in \mathbb{N}$. Olkoon $J_i = (I : \langle b^i \rangle)$. Koska

$$\cdots \subset \langle b^n \rangle \subset \cdots \subset \langle b^2 \rangle \subset \langle b \rangle,$$

voimme muodostaa nousevan ketjun ideaaleja

$$J_1 \subset J_2 \subset \cdots \subset J_k \subset \cdots$$

Ketjulla on maksimaalinen alkio J_n, sillä R on Noetherin rengas, eli kaikilla $m > n$ pätee $J_m = J_n$.

Olkoon $K = \langle b^n \rangle + I$. Osoitamme, että $I = J_n \cap K$. Nyt $I \subset J_n$, sillä $(I : J) = \{r \in R \mid rJ \subset I\}$. Selvästi kaikilla $r \in I$ pätee ehto. Lisäksi pätee selvästi $I \subset K$, eli $I \subset J_n \cap K$.

Otetaan alkio $r \in J_n \cap K$. Nyt on olemassa $s \in I$ ja $t \in R$ joilla $r = s + tb^n$, ja $rb^n \in I$. Edellinen seuraa siitä, että $J_n = (I : \langle b^n \rangle) = \{r \in R \mid r\langle b^n \rangle \subset I\}$, eli myös $rb^n \in I$. Nyt $rb^n = sb^n + tb^{2n}$, ja $t \in (I : \langle b^{2n} \rangle)$, mistä seuraa $t \in (I : \langle b^n \rangle)$. Edellisistä seuraa, että $r = s + tb^n \in I$, josta seuraa $J_n \cap K \subset I$.

Ideaalin I jaottomuuden nojalla pätee joko $I = J_n$ tai $I = K$. Käsittelemme molemmat vaihtoehdot.

- Jos $I = J_n = (I : \langle b^n \rangle)$, niin $I = (I : \langle b \rangle)$, sillä $I \subset (I : \langle b \rangle) \subset (I : \langle b^n \rangle)$. Oletimme alussa, että $ab \in I$, joten $a \in (I : \langle b \rangle) = I$.
- Jos $I = K = \langle b^n \rangle + I$, niin tällöin $b^n \in I$.

□

Lemma 5.0.12. *Jokainen ideaali Noetherin renkaassa R voidaan kirjoittaa äärellisenä leikkauksena jaottomista ideaaleista.*

Todistus. Olkoon S kaikkien renkaan R niiden ideaalien joukko, joita ei voi kirjoittaa äärellisenä leikkauksena jaottomista ideaaleista. Oletamme, että S on epätyhjä. Otamme mielivaltaisen nousevan ketjun $I_1 \subset I_2 \subset \cdots \subset I_n \cdots$. Tiedämme ketjulla olevan maksimaalisen alkion, sillä R on Noetherin rengas. Koska $I_n \in S$, se ei ole jaoton. Nyt on siis olemassa ideaalit J ja K, joilla pätee $I_n = J \cap K$. Nyt jos $J \in S$, I_n ei voisi olla ketjun maksimaalinen alkio, sillä selvästi $I_n \subset J$. Samalla tapaa näemme, että $K \notin S$. Joukon S määritelmän nojalla ideaalit J ja K olisivat molemmat jaottomien ideaalien äärellisiä leikkauksia, mutta koska määrittelimme $I_n = J \cap K$, myös I_n olisi jaottomien ideaalien äärellinen leikkaus. Löysimme ristiriidan, eli $S = \varnothing$. □

Esimerkki 5.0.13. Olkoon $x \in \mathbb{Z}$ mielivaltainen, ja tällä luvulla alkutekijähajotelma

$$x = \prod_{i=1}^{k} p_i^{a_i},$$

missä k on toisistaan eroavien alkutekijöiden määrä. Nyt luvun x virittämälle ideaalille pätee

$$\langle x \rangle = \bigcap_{i=1}^{k} \langle p_i^{a_i} \rangle.$$

Kokonaislukujen tapauksessa alkeishajotelma vastaa siis täysin aritmetiikan peruslausetta.

Esimerkki 5.0.14. Esimerkkiä 5.0.13 soveltaen. Tiedämme, että luvun 360 alkutekijähajotelma on $2^3 \cdot 3^2 \cdot 5$. Nyt pätee $\langle 360 \rangle = \{\cdots, -720, -360, 0, 360, 720, \cdots\}$. Lisäksi $\langle 8 \rangle = \{\cdots, -16, -8, 0, 8, 16, \cdots\}$, $\langle 9 \rangle = \{\cdots, -18, -9, 0, 9, 18, \cdots\}$ ja $\langle 5 \rangle = \{\cdots, -10, -5, 0, 5, 10, \cdots\}$. Näemme, että kolmen jälkimmäisen ideaalin yhteisiä alkioita ovat luvun 360 monikerrat, eli $\langle 360 \rangle = \langle 8 \rangle \cap \langle 9 \rangle \cap \langle 5 \rangle$.

Lause 5.0.15. *Olkoon R vaihdannainen Noetherin rengas ja I sen ideaali. Ideaali I on hajotettavissa äärellisen määrän alkeisideaaleja J_i leikkaukseksi, siis*

$$I = J_1 \cap J_2 \cap \cdots \cap J_n$$

Lisäksi jos poistaa minkä tahansa leikkauksen jäsenen J_k, niin leikkaus muuttuu, eli

$$J_1 \cap \cdots \cap \widehat{J_k} \cap \cdots \cap J_n \subsetneq I$$

Todistus. Lause seuraa suoraan lemmoista 5.0.11 ja 5.0.12.

□

Kirjallisuutta

[1] Herbert B. Enderton. *Elements of Set Theory.* Academic Press, 1977.

[2] Jokke Häsä. Algebra II, 2014.

[3] Jokke Häsä and Johanna Rämö. *Johdatus abstraktiin algebraan.* Gaudeamus Helsinki University Press, 2012.

[4] Serge Lang. *Algebra.* Graduate Texts in Mathematics. Springer New York, 2005.